Lawful basis for processing

Legitimate interests

ico.
Information Commissioner's Office

Legitimate interests

At a glance

- Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.
- It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
- Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.
- There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:
  - identify a legitimate interest;
  - show that the processing is necessary to achieve it; and
  - balance it against the individual's interests, rights and freedoms.
- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.
- Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy information.

Checklists

☐ We have checked that legitimate interests is the most appropriate basis.

☐ We understand our responsibility to protect the individual's interests.

☐ We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.

☐ We have identified the relevant legitimate interests.

☐ We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.

☐ We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.

☐ We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.

☐ We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.

☐ If we process children's data, we take extra care to make sure we protect their interests.

☐ We have considered safeguards to reduce the impact where possible.

☐ We have considered whether we can offer an opt out.

☐ If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.

☐ We keep our LIA under review, and repeat it if circumstances change.

☐ We include information about our legitimate interests in our privacy information.

In brief

What's new under the GDPR?

The concept of legitimate interests as a lawful basis for processing is essentially the same as the equivalent Schedule 2 condition in the 1998 Act, with some changes in detail.

You can now consider the legitimate interests of any third party, including wider benefits to society. And when weighing against the individual's interests, the focus is wider than the emphasis on 'unwarranted prejudice' to the individual in the 1998 Act. For example, unexpected processing is likely to affect whether the individual's interests override your legitimate interests, even without specific harm.

The GDPR is clearer that you must give particular weight to protecting children's data.

Public authorities are more limited in their ability to rely on legitimate interests, and should consider the 'public task' basis instead for any processing they do to perform their tasks as a public authority. Legitimate interests may still be available for other legitimate processing outside of those tasks.

The biggest change is that you need to document your decisions on legitimate interests so that you can demonstrate compliance under the new GDPR accountability principle. You must also include more information in your privacy information.

In the run up to 25 May 2018, you need to review your existing processing to identify your lawful basis and document where you rely on legitimate interests, update your privacy information, and communicate it to individuals.

What is the 'legitimate interests' basis?

Article 6(1)(f) gives you a lawful basis for processing where:

> "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

This can be broken down into a three-part test:

1. **Purpose test:** are you pursuing a legitimate interest?
2. **Necessity test:** is the processing necessary for that purpose?
3. **Balancing test:** do the individual's interests override the legitimate interest?

A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test.

The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. It also says that you have a legitimate interest in disclosing information about possible criminal acts or security threats to the authorities.

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You cannot rely on legitimate interests if there is another reasonable and less intrusive way to achieve the same result.

You must balance your interests against the individual's interests. In particular, if they would not reasonably expect you to use data in that way, or it would cause them unwarranted harm, their interests are likely to override yours. However, your interests do not always have to align with the individual's interests. If there is a conflict, your interests can still prevail as long as there is a clear justification for the impact on the individual.

When can we rely on legitimate interests?

Legitimate interests is the most flexible lawful basis, but you cannot assume it will always be appropriate for all of your processing.

If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected.

Legitimate interests is most likely to be an appropriate basis where you use data in ways that people

would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified.

You can rely on legitimate interests for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object – but only if you don't need consent under PECR. See our Guide to PECR for more on when you need consent for electronic marketing.

You can consider legitimate interests for processing children's data, but you must take extra care to make sure their interests are protected. See our detailed guidance on children and the GDPR.

You may be able to rely on legitimate interests in order to lawfully disclose personal data to a third party. You should consider why they want the information, whether they actually need it, and what they will do with it. You need to demonstrate that the disclosure is justified, but it will be their responsibility to determine their lawful basis for their own processing.

You should avoid using legitimate interests if you are using personal data in ways people do not understand and would not reasonably expect, or if you think some people would object if you explained it to them. You should also avoid this basis for processing that could cause harm, unless you are confident there is nevertheless a compelling reason to go ahead which justifies the impact.

If you are a public authority, you cannot rely on legitimate interests for any processing you do to perform your tasks as a public authority. However, if you have other legitimate purposes outside the scope of your tasks as a public authority, you can consider legitimate interests where appropriate. This will be particularly relevant for public authorities with commercial interests.

See our guidance page on the lawful basis for more information on the alternatives to legitimate interests, and how to decide which basis to choose.

How can we apply legitimate interests in practice?

If you want to rely on legitimate interests, you can use the three-part test to assess whether it applies. We refer to this as a legitimate interests assessment (LIA) and you should do it before you start the processing.

An LIA is a type of light-touch risk assessment based on the specific context and circumstances. It will help you ensure that your processing is lawful. Recording your LIA will also help you demonstrate compliance in line with your accountability obligations under Articles 5(2) and 24. In some cases an LIA will be quite short, but in others there will be more to consider.

First, identify the legitimate interest(s). Consider:

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

Second, apply the necessity test. Consider:

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Third, do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are you processing children's data?
- Are any of the individuals vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

You then need to make a decision about whether you still think legitimate interests is an appropriate basis. There's no foolproof formula for the outcome of the balancing test – but you must be confident that your legitimate interests are not overridden by the risks you have identified.

Keep a record of your LIA and the outcome. There is no standard format for this, but it's important to record your thinking to help show you have proper decision-making processes in place and to justify the outcome.

Keep your LIA under review and refresh it if there is a significant change in the purpose, nature or context of the processing.

If you are not sure about the outcome of the balancing test, it may be safer to look for another lawful basis. Legitimate interests will not often be the most appropriate basis for processing which is unexpected or high risk.

If your LIA identifies significant risks, consider whether you need to do a DPIA to assess the risk and potential mitigation in more detail. See our guidance on DPIAs for more on this.

What else do we need to consider?

You must tell people in your privacy information that you are relying on legitimate interests, and explain what these interests are.

If you want to process the personal data for a new purpose, you may be able to continue processing under legitimate interests as long as your new purpose is compatible with your original purpose. We would still recommend that you conduct a new LIA, as this will help you demonstrate compatibility.

If you rely on legitimate interests, the right to data portability does not apply.

If you are relying on legitimate interests for direct marketing, the right to object is absolute and you must stop processing when someone objects. For other purposes, you must stop unless you can show that your legitimate interests are compelling enough to override the individual's rights. See our guidance on individual rights for more on this.

Further Reading

Relevant provisions in the GDPR - See Article 6(1)(f) and Recitals 47, 48 and 49
External link

In more detail – ICO guidance

We have produced more detailed guidance on legitimate interests

In more detail - Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

There are no immediate plans for Article 29 Working Party guidance on legitimate interests under the GDPR, but WP29 Opinion 06/2014 (9 April 2014) gives detailed guidance on the key elements of the similar legitimate interests provisions under the previous Data Protection Directive 95/46/EC.

About this detailed guidance

About this detailed guidance

These pages sit alongside our Guide to the GDPR and provide more detailed guidance for UK organisations on legitimate interests under the GDPR.

This guidance will help you to decide when to rely on legitimate interests as your basis for processing personal data and when to look at alternatives. It explains when using legitimate interests as a lawful basis is appropriate, what it means, and how to decide whether it applies to your particular processing operation.

The concept of 'legitimate interests' also appears in connection with international transfers (Article 49). However this guidance focuses on legitimate interests in its role as a lawful basis in Article 6.

For an introduction to the key themes and provisions of the GDPR, you should refer back to the guide. You can navigate back to the guide at any time using the link at the top of this page. Links to other relevant guidance and sources of further information are also provided throughout.

When downloading this guidance, the corresponding content from the Guide to the GDPR will also be included so you will have all the relevant information on this topic.

What's new under the GDPR?

In detail

Is this a big change?

No. The role of legitimate interests as a potential lawful basis (or condition) for processing is not new. Legitimate interests was one of the conditions for processing under the 1998 Act and the wording of this provision is similar:

1998 Act:

"The processing is necessary for the purposes of legitimate interests pursued by the data controller…

…or by the third party or parties to whom the data are disclosed, …

…except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject."

GDPR:

"processing is necessary for the purposes of the legitimate interests pursued by the controller…

…or by a third party, …

…except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

There are some differences in wording, but the three key elements of the concept of legitimate interests remain the same:

- a legitimate interest;
- a necessity test;
- a balance with individuals' interests, rights and freedoms.

The main changes instead arise out of the way legitimate interests interacts with new accountability and transparency requirements. There is also a bigger change for public authorities, who are more restricted in when they can rely on legitimate interests.

How is the wording different?

While the key elements remain the same, there are some small changes to the detail.

Legitimate interests that are relevant are no longer limited to your own interests or those of third parties to whom you disclose the data. You can now consider the interests of any third party, including the wider benefits to society.

Under the 1998 Act, the processing impact had to be unwarranted due to prejudice to the individual's interests before it would override your legitimate interests, ie the provision implied a focus on demonstrable harm. However, prejudice is not a term used in the GDPR version of the provision, and it's clear that this is intended to be wider than a pure harm-based assessment. For example, Recital 47 indicates that if the individual does not reasonably expect the processing, their rights may override your legitimate interests.

The provision also highlights children's data as requiring special consideration. If your processing includes children's personal data, you must give particular weight to protecting their data and ensure that you properly consider their interests and their rights and freedoms. For further information see the section on children's personal data and legitimate interests.

What else is new?

The GDPR brings in new accountability and transparency requirements.

Under the new accountability principle you need to be able to show that you have a lawful basis for each processing operation. If you are relying on legitimate interests, you need to document your assessment of how it applies to the particular processing, and ensure that you can justify your decision if necessary.

As the application of legitimate interests is not always self-evident, documenting your assessment of legitimate interests is particularly important in helping you to demonstrate compliance under the accountability principle.

Under transparency requirements you must inform individuals upfront which lawful basis you are relying on. If you are relying on legitimate interests as your basis, you must also tell individuals what these legitimate interests are. See the section on what do we need to tell people for further information.

The ability of public authorities to rely on legitimate interests is more limited under the GDPR – for more information see the section on can public authorities use legitimate interests.

Further Reading

> Relevant provisions in the GDPR – See Article 6(1)(f), Article 13(1)(c) and (d), Article 14(1)(c) and (2)(b) and Article 5(2) and Article 24
> External link

What are the key steps to take to prepare for the GDPR?

You must ensure that you bring any processing of personal data already underway into conformity with the GDPR prior to 25 May 2018. As part of this exercise, you need to review your existing processing operations and conditions for processing, and take steps to ensure that you meet the accountability and transparency requirements of the GDPR.

If you were relying on legitimate interests as your condition for processing under the 1998 Act, in many cases you are able to continue to rely on this as your basis for processing under the GDPR.

However you must check whether legitimate interests remains the most suitable basis for your processing. This is your chance to ensure that you have selected the most appropriate basis (or bases). If you find at a later date that the legitimate interests basis was inappropriate, it is difficult to retrospectively swap to a different basis that you did not initially identify as this would lead to breaches of the accountability and transparency provisions.

If you wish to continue relying on legitimate interests, you need to make sure that you can demonstrate that it applies, in line with the approach set out in this guidance.

In order to the meet the accountability requirements you should document your decision and the factors you took into account.

You must also update your privacy information to clearly say that you are relying on legitimate interests as your lawful basis, and say what your legitimate interests are.

Further Reading

> Relevant provisions in the GDPR – See Articles 13(1)(c), 13(1)(d), 14(1)(c), 14(2)(b) and Article 5(2) and Article 24
> External link

Further reading - ICO guidance

Lawful basis for processing

Right to be informed

Can we move to legitimate interests from a different basis under the 1998 Act?

Yes. If you discover that your existing basis (or condition) for processing under the 1998 Act is inappropriate under the GDPR, or you decide that legitimate interests is actually more appropriate, then you can choose to swap to legitimate interests.

If for example you have been processing on the basis of consent but you find that your existing consents do not meet the GDPR standard, and you do not wish to seek fresh GDPR-compliant consent, you may be able to consider legitimate interests instead. However you must be confident that you want to take responsibility for demonstrating that your processing is in line with people's reasonable expectations and that it wouldn't have an unjustified impact on them.

You must still ensure that your processing is fair. If you wish to move from consent under the 1998 Act to legitimate interests under the GDPR, you need to ensure that you clearly inform individuals of the change in your privacy notice. To ensure there is no unjustified impact on their rights, you should consider giving them a clear chance to opt out, and retaining any preference controls that were in place.

You also need to inform individuals of their right to object to processing based on legitimate interests (although this is not an absolute right in most cases).

What is the ‘legitimate interests’ basis?

In detail

What does Article 6(1)(f) say about legitimate interests?

Legitimate interests is one of the six lawful bases for processing personal data. You must have a lawful basis in order to process personal data in line with the ‘lawfulness, fairness and transparency’ principle.

Article 6(1)(f) states:

> “1.Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

Legitimate interests is different to the other lawful bases as it is not centred around a particular purpose (eg performing a contract with the individual, complying with a legal obligation, protecting vital interests or carrying out a public task), and it is not processing that the individual has specifically agreed to (consent). Legitimate interests is more flexible and could in principle apply to any type of processing for any reasonable purpose.

Because it could apply in a wide range of circumstances, it puts the onus on you to balance your legitimate interests and the necessity of processing the personal data against the interests, rights and freedoms of the individual taking into account the particular circumstances. This is different to the other lawful bases, which presume that your interests and those of the individual are balanced.

The key elements of the legitimate interests provision can be broken down into a three-part test.

Further Reading

Relevant provisions in the GDPR – See Article 6(1)(f) and Recital 47
External link

Further reading – ICO guidance

Lawful basis for processing

What is the three-part test?

Whilst a three-part test is not explicitly set out as such in the GDPR, the legitimate interests provision does incorporate three key elements. Article 6(1)(f) breaks down into three parts:

> "processing is necessary for…
>
> …the purposes of the legitimate interests pursued by the controller or by a third party, …
>
> …except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

It makes most sense to apply this as a test in the following order:

- **Purpose test** – is there a legitimate interest behind the processing?
- **Necessity test** – is the processing necessary for that purpose?
- **Balancing test** – is the legitimate interest overridden by the individual's interests, rights or freedoms?

This concept of a three-part test for legitimate interests is not new. In fact the Court of Justice of the European Union confirmed this approach to legitimate interests in the Rigas case (C-13/16, 4 May 2017) in the context of the Data Protection Directive 95/46/EC, which contained a very similar provision.

This means it is not sufficient for you to simply decide that it's in your legitimate interests and start processing the data. You must be able to satisfy all three parts of the test prior to commencing your processing.

Further Reading

Relevant provisions in the GDPR – See Article 6(1)(f)
External link

What counts as a 'legitimate interest'?

A wide range of interests may be legitimate interests. It could be your legitimate interests in the processing or it could include the legitimate interests of any third party. The term 'third party' doesn't just refer to other organisations, it could also be a third party individual.

The legitimate interests of the public in general may also play a part when deciding whether the legitimate interests in the processing override the individual's interests and rights. If the processing has a wider public interest for society at large, then this may add weight to your interests when balancing these against those of the individual.

Example

An insurance company wants to process personal data to spot fraudulent claims on the basis of legitimate interests.

Firstly it considers the purpose test. It is in the company's legitimate business interests to ensure that its customers do not defraud it out of money. However at the same time the company's other customers and the public in general also have a legitimate interest in ensuring that fraud is prevented and detected.

As it has met the purpose test the insurance company can then go onto consider the necessity test and then the balancing test.

The GDPR does not define what factors to take into account when deciding if your purpose is a legitimate interest. It could be as simple as it being legitimate to start up a new business activity, or to grow your business.

Because the term 'legitimate interest' is broad, the interests do not have to be very compelling (although in some instances they may be) and it does not rule out interests that are more trivial. An interest that could be seen as trivial or controversial could still be a legitimate interest for these purposes, although be aware they are more easily overridden in the balancing test or if the data subject objects under Article 21.

Showing that you have a legitimate interest does mean however that you (or a third party) must have some clear and specific benefit or outcome in mind. It is not enough to rely on vague or generic business interests. You must think about specifically what you are trying to achieve with the particular processing operation.

For example, it is not enough to simply say: 'we have a legitimate interest in processing customer data', as this does not clarify your purpose or intended outcome. Instead, you need to be more specific about your purpose, such as: 'we have a legitimate interest in marketing our goods to existing customers to increase sales'.

Whilst any purpose could potentially be relevant, that purpose must be 'legitimate'. Anything illegitimate, unethical or unlawful is not a legitimate interest. For example, although marketing may in general be a legitimate purpose, sending spam emails in breach of electronic marketing rules is not legitimate.

If the interest is not legitimate then you do not meet the first part of the test and you are not able to use legitimate interests as your lawful basis. There is no need to consider the rest of the test as the other parts are not able to legitimise processing that is illegitimate from the outset.

The GDPR does not have an exhaustive list of what purposes are likely to constitute a legitimate interest. However, the recitals do say the following purposes constitute a legitimate interest:

- fraud prevention;
- ensuring network and information security; or
- indicating possible criminal acts or threats to public security.

Therefore, if you are processing for one of these purposes you may have less work to do to show that the legitimate interests basis applies.

The recitals also say that the following activities may indicate a legitimate interest:

- processing employee or client data;
- direct marketing; or
- administrative transfers within a group of companies.

However, whilst these last three activities may indicate a legitimate interest, you still need to do some work to identify your precise purpose and show that it is legitimate in the specific circumstances, and in particular that any direct marketing complies with e-privacy rules on consent. You would also need to go on to assess the rest of the three-part test. See When can we rely on legitimate interests? for more information on the impact of these recitals.

These examples of processing highlighted by the GDPR recitals are not exhaustive. You may also be able to demonstrate in a wide range of other situations that you are processing for the purposes of legitimate interests.

For more practical steps on how to assess the purpose test and document your legitimate interests, read How do we apply legitimate interests in practice?.

Further Reading

> Relevant provisions in the GDPR – See Article 6(1)(f) and Recitals 47, 48, 49, and 50 (external link)
> External link

Further reading – ICO guidance

Right to object

When is processing 'necessary'?

You need to demonstrate that the processing is **necessary** for the purposes of the legitimate interests you have identified. This doesn't mean that it has to be absolutely essential, but it must be a targeted and proportionate way of achieving your purpose.

You need to decide on the facts of each case whether the processing is proportionate and adequately targeted to meet its objectives, and whether there is any less intrusive alternative, ie can you achieve

your purpose by some other reasonable means without processing the data in this way? If you could achieve your purpose in a less invasive way, then the more invasive way is not necessary.

Example

An organisation undertakes work that is particularly sensitive so it wants to ensure that the individuals it employs have been vetted. It decides to make its job offers conditional on the individual having vetting or background checks.

In the purpose test, the organisation determines that it is in its legitimate business interests to have fully vetted staff given the nature of the work. It considers the different roles that it has and determines that the level of vetting would be different depending on the type of role. It assesses what checks and vetting are actually necessary for each role to ensure that the processing is targeted and proportionate to the specific role and responsibilities in order to meet the necessity test.

If the processing includes criminal offence data the organisation would also need to have a separate condition for processing this data in compliance with Article 10.

Example

A public figure posts a video about overcrowding on trains that shows them on a train run by a particular train operator. The video is reported on by various media outlets.

The train operator wants to release the CCTV footage of the public figure on the train in order to counter the reports that the train was overcrowded. The footage it holds also includes images of other passengers.

The train operator has a legitimate interest in releasing the footage in order to correct what it deems to be misleading news reports that are potentially damaging to its reputation and commercial interests.

It considers the necessity test and concludes that it is not possible to achieve its legitimate interests without publishing the image of the public figure as it can only counter the existing news footage to show that there were empty seats on the train if it shows the public figure on that journey.

However whilst it is able to demonstrate that it is necessary to publish the public figure’s image in order pursue its legitimate interests (ie to give its side of the story), it is not necessary for the train operator to publish pictures of anyone else on the train.

It needs therefore to take steps to ensure that the images of passengers other than the public figure are obscured, as well as going on to consider the balancing test.

You should be careful not to confuse processing that is necessary for your stated purpose with processing which is only necessary because of your chosen method of pursuing that purpose. In the

context of legitimate interests, you may be able to argue that some non-essential features of your processing (such as profiling or marketing) are necessary for your purposes. However, this is only the case if you clearly identify the specific purpose behind those particular features, and don't hide behind a vague business objective that could be achieved in another way. The processing must be necessary for the specific purpose you have identified in step one. This is one reason why it is important to be clear and specific about your purposes.

If you are unable to demonstrate that the processing actually helps meet the legitimate interest, then you are not able to apply this basis. Likewise if the processing is not a reasonable way to achieve your stated purpose then legitimate interests does not apply. If there is another reasonable and less invasive way to meet the interest and achieve your purpose without the processing, then it would be unlawful (unless another lawful basis applies).

For more practical steps on assessing and documenting the necessity test, see the section on How do we apply legitimate interests in practice?.

Further reading – ICO guidance

Criminal offence data

What is the balancing test?

Just because you have determined that your processing is necessary for a legitimate interest does not mean that you are automatically able to rely on this basis for processing. You must also perform a 'balancing test' to justify any impact on individuals.

The balancing test is where you take into account "the interests or fundamental rights and freedoms of the data subject which require the protection of personal data", and check they don't override your interests. In essence, this is a light-touch risk assessment to check that any risks to individuals' interests are proportionate.

If the data belongs to children then you need to be particularly careful to ensure their interests and rights are protected.

What are the individual's 'interests, rights and freedoms'?

The interests, rights and freedoms of individuals in this context is a broad concept which includes data protection and privacy rights, but also other fundamental rights as well as more general interests.

It is clear from other related provisions in the GDPR which talk about risks to the rights and freedoms of individuals that the focus here should be on any potential impact on individuals. Recital 75 provides some relevant guidance here. It makes clear that a risk to individuals' rights and freedoms is about the potential for any type of impact. This includes physical, financial or any other impact, such as:

- inability to exercise rights (including data protection rights);
- loss of control over the use of personal data; or
- any social or economic disadvantage.

Further Reading

Relevant provisions in the GDPR – See Article 6(1)(f), and Recitals 47 and 75
External link

What is the importance of reasonable expectations?

The GDPR is clear that the interests of the individual could in particular override your legitimate interests if you intend to process personal data in ways the individual does not reasonably expect. This is because if processing is unexpected, individuals lose control over the use of their data, and may not be in an informed position to exercise their rights. There is a clear link here to your transparency obligations.

Recital 47 says:

> "At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing."

You need to assess whether the individual can reasonably expect the processing, taking into account in particular when and how the data was collected.

This is an objective test. The question is not whether a particular individual actually expected the processing, but whether a reasonable person should expect the processing in the circumstances.

One of the factors that may affect what individuals reasonably expect is what you tell them in your privacy information. If you include clear information about your processing, they are more likely to expect that processing.

Your relationship with the individual also plays a part in determining whether the individual would reasonably expect the processing to occur. Recital 47 indicates that legitimate interests is more likely to apply where you have a 'relevant and appropriate relationship', for example, because they are your client or employee. If you don't have a pre-existing relationship, it is harder to demonstrate that the processing can be reasonably expected. If you obtained the data from a third party, you need to be clear what the individual was told about when that data might be passed on for use by others, and whether this covers you and your purpose for processing, as this will affect reasonable expectations.

Other factors might also affect the reasonable expectations of individuals, such as:

- how long ago you collected the data;
- the source of the data;
- the precise nature of any existing relationship with the individual and how you have used their data in the past; and
- whether you are using a new technology or processing data in a new way that individuals have not anticipated – or conversely whether there are any developments in technology or updates to services

which individuals have come to expect.

Example

An individual uploads their CV to a jobs board website. A recruitment agency accesses the CV and thinks that the individual may have the skills that two of its clients are looking for and wants to pass the CV to those companies.

It is likely in this situation that the lawful basis for processing for the recruitment agency and their clients is legitimate interests.

The individual has made their CV available on a job board website for the express reason of employers being able to access this data. They have not given specific consent for identified data controllers, but they would clearly expect that recruitment agencies would access the CV and share with it their clients, indeed, this is likely to be the individual's intention. As such, the legitimate interest of the recruitment agencies and their clients to fill vacancies would not be overridden by any interests or rights of the individual. In fact, those legitimate interests are likely to align with the interests of the individual in circulating their CV in order to find a job.

Example

An individual creates a profile on a social networking website designed specifically for professional networking. There is a specific option to select a function to let recruiters know that the individual is open to job opportunities.

If the individual chooses to select that option, they would clearly expect those who view their profile might use their contact details for recruitment purposes and legitimate interests may be available (subject to compliance with other legal requirements, and PECR in particular). However, if they choose not to select that option, there is no such expectation, and their interests in maintaining control over their data overrides any legitimate interests of a recruitment agency or recruiting organisation.

Although reasonable expectations is an important factor, it does not automatically determine the outcome. Simply having warned the individual in advance that their data will be processed in a certain way does not necessarily mean that your legitimate interests always prevail, irrespective of harm. And in some cases you may still be able to justify unexpected processing if you have a compelling reason for it.

When do individuals' interests override ours?

Even if the processing might have a negative impact on the individual, this does not automatically mean that their interests always override yours. This depends on the severity of the impact, and whether it is warranted in light of your purpose. Your interests do not always have to be in harmony with those of the

individual, and if you have a more compelling interest this may justify some impact on individuals.

Example

A finance company is unable to locate a customer who has stopped making payments under a hire purchase agreement. The customer has moved house without notifying the finance company of their new address. The finance company wants to engage a debt collection agency to find the customer and seek repayment of the debt. It wants to disclose the customer's personal data to the agency for this purpose.

The finance company has a legitimate interest in recovering the debt it is owed and in order to achieve this purpose it is necessary for them to use a debt collection agency to track down the customer for payment owed.

The finance company considers the balancing test and concludes that it is reasonable for its customers to expect that they will take steps to seek payment of outstanding debts. It is clear that the interests of the customer are likely to differ from those of the finance company in this situation, as it may suit the customer to evade paying their outstanding debt.

However, the legitimate interest in passing the personal data to a debt collection agency in these circumstances would not be overridden by the interests of the customer. The balance would be in favour of the finance company.

However, if there is a serious mismatch between your interests and those of the individual (whose are stronger), the individual's interests come first, for example where:

- they would not reasonably expect the processing;
- they would be likely to object to the processing;
- the processing would have a significant impact on them;
- the processing would prevent them exercising their rights; or
- the data you are processing is particularly sensitive, for example special category data, criminal offence data, or children's data.

However the outcome will depend on the circumstances of the case.

For more practical guidance on how to assess the balancing test, read the section on How do we apply legitimate interests in practice?.

When can we rely on legitimate interests?

In detail

When might legitimate interests be appropriate?

Legitimate interests is the most flexible of the six lawful bases. It is not focused on a particular purpose and therefore gives you more scope to potentially rely on it in many different circumstances.

It may be the most appropriate basis when:

- the processing is not required by law but is of a clear benefit to you or others;
- there's a limited privacy impact on the individual;
- the individual should reasonably expect you to use their data in that way; and
- you cannot, or do not want to, give the individual full upfront control (ie consent) or bother them with disruptive consent requests when they are unlikely to object to the processing.

There may also be occasions when you have a compelling justification for the processing which may mean that a more intrusive impact on the individual can be warranted. However in such cases you need to ensure that you can demonstrate that any impact is justified.

The legitimate interests basis is likely to be most useful where there is either a minimal impact on the individual, or else a compelling justification for the processing.

Can we use it as the default basis for all of our processing?

No. Although legitimate interests is a flexible concept and will often be relevant, it does not apply to everything and you are not be able to use it as the default basis for all your processing.

None of the lawful bases take precedence over the others, and you should always use the one that is most appropriate to the circumstances having considered the purpose of the processing.

You should carefully consider whether legitimate interests is the appropriate lawful basis for the particular processing operation. You should not look to rely on it simply because it may initially seem easier to apply than other lawful bases. It is not always be the easiest option, and in fact places more responsibility on you to justify your processing and any impact on individuals. In effect, it requires a risk assessment based on the specific context and circumstances to demonstrate that processing is appropriate.

Further reading – ICO guidance

Lawful basis for processing guidance

What are the benefits of choosing legitimate interests?

Because this basis is not purpose-specific, it is particularly flexible and it may be applicable in a wide range of different situations. It can also give you more ongoing control and security over your long-term processing than consent, where an individual could withdraw their consent at any time. Although remember that you still have to consider objections.

It also promotes a risk-based approach to compliance as you need to think about the impact of your processing on individuals, which can help you identify risks and take appropriate safeguards. This can also support your obligation to ensure 'data protection by design', and help you identify when you might need to do a data protection impact assessment (DPIA).

Using this basis for processing that is expected and has a low privacy impact may help you avoid bombarding people with unnecessary consent requests and can help avoid 'consent fatigue'. It can also, if done properly, be an effective way of protecting the individual's interests, especially when combined with clear privacy information and an upfront opportunity to opt out.

Are there any disadvantages?

You may find there is more work for you to do to justify the application of legitimate interests compared to some of the other lawful bases. For example, the other lawful bases which incorporate a necessity test specify the purpose of the processing. However, legitimate interests gives you the job of explaining your purpose and justifying why this is in your legitimate interests in addition to you having to demonstrate the necessity of the processing. The onus is also on you to ensure – and demonstrate – that your interests are balanced with the individual.

It may be harder to demonstrate compliance as there is more scope for disagreement over the outcome of the balancing test. You need to be able to clearly justify your decision that the balance actually favours you processing the data.

If you intend to rely on legitimate interests you need to be confident about taking on the responsibility of protecting the interests of the individual. If it is more appropriate to put the onus on individuals to take responsibility for the use of their data, then you may wish to consider whether consent would be a more appropriate lawful basis.

You also need to do more work to be transparent when you are relying on legitimate interests. You need to clearly explain in your privacy policy what the legitimate interests of the processing are.

Further Reading

Relevant provisions in the GDPR – See Article 6(1)(f) and Article 6(1)(a)
External link

Further reading – ICO guidance

Consent

Can public authorities use legitimate interests?

Yes, in some instances public authorities are able to consider using legitimate interests as a lawful basis.

However, if you are a public authority you cannot use legitimate interests as your lawful basis if the processing is in the performance of your tasks as a public authority. The GDPR explains the reason for this exclusion is because it is for the legislature to give public authorities the legal authority to process personal data; ie if you are a public authority you should only be able to process personal data in performance of your tasks if the law has given you authorisation.

Other lawful bases are available to you if you are a public authority and these are likely to be more appropriate for some types of processing that you undertake; eg if you are performing your tasks you should instead consider the 'public task' basis.

Whilst you cannot use legitimate interests as a basis when processing for your tasks as a public authority, this does not mean that it can never apply.

This restriction on the use of legitimate interests is about the nature of the task, not the nature of the organisation. This means that if you are a public authority legitimate interests could potentially be available for you to rely on if you can demonstrate that the processing is not part of you performing your tasks as a public authority.

Further Reading

Relevant provisions in the GDPR – See Articles 6(1)(f) and Recitals 47
External link

Further reading – ICO guidance

Public task

Are there cases when the purpose will constitute a legitimate interest?

The GDPR highlights certain purposes that either 'constitute' a legitimate interest or 'should be regarded as' a legitimate interest. These are:

- fraud prevention;
- network and information security; and
- indicating possible criminal acts or threats to public security.

If you are processing for these purposes then you will have met the purpose test and if you can show your processing is necessary (or in some cases 'strictly' necessary), then this can make the balancing test more straightforward. Processing for these purposes is a strong factor in the balancing test therefore, depending on the circumstances, your balancing test could be brief.

Whilst processing for these purposes is likely to make it easier to rely on the basis of legitimate interests, you still need to consider your wider compliance with other GDPR obligations and safeguards. For example, Article 9 conditions if you are processing special category data, Article 10 if you are processing criminal offence data, transparency requirements, data minimisation, and any obligation to carry out a DPIA.

Are there cases when legitimate interests is likely to apply?

The GDPR highlights some processing activities where the legitimate interests basis is likely to apply:

- processing employee or client data;
- direct marketing; or
- intra-group administrative transfers.

The recitals say that legitimate interests 'may' apply to these processing activities, but this does not mean these activities will always be a legitimate interest or it automatically gives you a lawful basis for processing. You still need to apply the three-part test to demonstrate that it does apply in the particular circumstances.

Can we use legitimate interests for employee or client data?

Yes, in some cases, but it does not always apply and you need to consider the three-part test. Recital 47 of the GDPR says:

> "…Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller."

This means that a legitimate interest **could exist** where there is a 'relevant and appropriate relationship' between you and the individual. For example if the individual is your client or your employee. However it does not say that the legitimate interests basis always applies.

It may be more likely to apply because you are more likely to have an evident legitimate purpose for using this data, and the nature of your relationship means the processing is less likely to be unexpected or unwanted, so the balancing test is likely to be easier.

In some instances it may be that your interests and those of the individual are actually aligned or intertwined. For example you are supporting staff development or dealing with the needs of a customer. However this does not mean that when there's an appropriate relationship there's automatically a mutual legitimate interest.

You still need to specify your interests, demonstrate that the processing is necessary and consider the balancing test.

There is likely to be some overlap with personal data processed on the basis of performance of a contract. If the processing is actually necessary for you to perform your side of a contract with the employee or client, then you should consider Article 6(1)(b) instead.

Further reading – ICO guidance

Lawful basis for processing – Contract

Can we use legitimate interests for intra-group transfers?

Yes, in some cases, but again, it does not automatically cover all such processing and you need to consider the three-part test. Recital 48 says:

> "Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected."

This indicates that you **may have** a legitimate interest in transmitting personal data to other organisations within your group for administrative purposes. But it does not say this always constitutes a

legitimate interest. If you operate within a group of entities and subsidiaries then you may be able to demonstrate that transfers within the group are necessary for a legitimate interest of group administration, but you need to identify your specific purpose, show that the processing of this data is necessary for that purpose, and consider the balancing test.

Example

Company AAA is a subsidiary of Company A. Company AAA does not have a HR department as this function is performed centrally at Company A. Company AAA wants to rely on legitimate interests as their lawful basis for passing employee data to Company A.

Company AAA concludes that it is in its legitimate interests to disclose information about leave, sickness, performance etc to its parent company for efficient group HR administration purposes.

Company AAA however needs to consider whether transferring this data is actually necessary for this purpose, and then balance this against the interests of the individuals, before they can be sure that the processing is lawful on the basis of legitimate interests.

As the data that Company AAA wants to transfer includes special category data, it also needs to identify a special category condition for processing in compliance with Article 9.

It is important to note that whilst you may consider that legitimate interests gives you a lawful basis for the transfer, the rules on transferring personal data to a company in a third country still apply. You still need to ensure that you comply with international transfers requirements.

Further Reading

Relevant provisions in the GDPR – See Recital 47, Recital 48, Recital 49, Recital 50 and Article 6(1)(b) (contracts) and Chapter V (international transfers)
External link

Further reading – ICO guidance

International transfers

Special category data

Can we use legitimate interests for our marketing activities?

Yes, in some cases, but you need to apply the three-part test and ensure that you comply with other marketing laws. Recital 47 of the GDPR says:

> "…The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

This means that direct marketing **may** be a legitimate interest. However the GDPR does not say that direct marketing always constitutes a legitimate interest, and whether your processing is lawful on the basis of legitimate interests depends on the particular circumstances.

In terms of the purpose test, some forms of marketing may not be legitimate if they do not comply with other legal or ethical standards or with industry codes of practice. However, as long as the marketing is carried out in compliance with e-privacy laws and other legal and industry standards, in most cases it is likely that direct marketing is a legitimate interest.

However this does not automatically mean that all processing for marketing purposes is lawful on this basis. You still need to show that your processing passes the necessity and balancing tests.

You may also need to be more specific about your purposes for some elements of your processing in order to show that processing is necessary and to weigh the benefits in the balancing test. For example, if you use profiling to target your marketing.

It is sometimes suggested that marketing is in the interests of individuals, for example if they receive money-off products or offers that are directly relevant to their needs. This is unlikely however to add much weight to your balancing test, and we recommend you focus primarily on your own interests and avoid undue focus on presumed benefits to customers unless you have very clear evidence of their preferences.

In some cases marketing has the potential to have a significant negative effect on the individual, depending on their personal circumstances. For example, someone known or likely to be in financial difficulties who is regularly targeted with marketing for high interest loans may sign up for these offers and potentially incur further debt.

When looking at the balancing test, you should also consider factors such as:

- whether people would expect you to use their details in this way;
- the potential nuisance factor of unwanted marketing messages; and
- the effect your chosen method and frequency of communication might have on more vulnerable individuals.

Given that individuals have the absolute right to object to direct marketing under Article 21(2), it is more difficult to pass the balancing test if you do not give individuals a clear option to opt out of direct marketing when you initially collect their details (or in your first communication, if the data was not collected directly from the individual). The lack of any proactive opportunity to opt out in advance would arguably contribute to a loss of control over their data and act as an unnecessary barrier to exercising their data protection rights.

Example

A charity wants to send fundraising material by post to individuals who have donated to them in the past but have not previously objected to receiving marketing material from them.

The charity's purpose of direct marketing to seek funds to further its cause is a legitimate interest.

The charity then looks at whether sending the mailing is necessary for its fundraising purpose. It decides that it is necessary to process contact details for this purpose, and that the mailing is a proportionate way of approaching individuals for donations.

The charity considers the balancing test and takes into account that the nature of the data being processed is names and addresses only, and that it would be reasonable for these individuals to expect that they may receive marketing material by post given their previous relationship.

The charity determines that the impact of a fundraising mailing on these individuals is likely to be minimal however it includes details in the mailing (and each subsequent one) about how individuals can opt out of receiving postal marketing in future.

If you intend to process personal data for the purposes of direct marketing by electronic means (by email, text, automated calls etc) legitimate interests may not always be an appropriate basis for processing. This is because the e-privacy laws on electronic marketing – currently the Privacy and Electronic Communications Regulations (PECR) – require that individuals give their consent to some forms of electronic marketing. It is the GDPR standard of consent that applies, because of the effect of Article 94 of the GDPR.

If e-privacy laws require consent, then processing personal data for electronic direct marketing purposes is unlawful under the GDPR without consent. If you have not got the necessary consent, you cannot rely on legitimate interests instead. You are not able to use legitimate interests to legitimise processing that is unlawful under other legislation.

If you have obtained consent in compliance with e-privacy laws, then in practice consent is also the appropriate lawful basis under the GDPR. Trying to apply legitimate interests when you already have GDPR-compliant consent would be an entirely unnecessary exercise, and would cause confusion for individuals.

If e-privacy laws do not require consent, legitimate interests may well be appropriate. Based on the current legislation (PECR), and depending on the outcome of your three-part test, legitimate interests may be appropriate for 'solicited' marketing (ie marketing proactively requested by the individual), or for unsolicited marketing in the following circumstances:

Marketing method	**Is legitimate interests likely to be appropriate?**
Post	✓
'Live' phone calls to TPS/CPTS registered numbers	✗
'Live' phone calls to those who have objected to your calls	✗
'Live' phone calls where there is no TPS/CTPS registration or objection	✓

Automated phone calls	✗
Emails/text messages to individuals – obtained using 'soft opt-in'	✓
Emails/text messages to individuals – without 'soft opt-in'	✗
Emails/text messages to business contacts	✓

You also need to remember that Article 21 specifically gives the data subject the right to object to processing of their personal data for the purposes of direct marketing, and you must inform them of that right. If the data subject objects then this overrides your legitimate interests and you need to stop processing their data for direct marketing purposes.

The EU is in the process of replacing the current e-privacy law (and therefore PECR) with a new ePrivacy Regulation (ePR). However the new ePR is yet to be agreed. The existing PECR rules continue to apply until the ePR is finalised, with some changes for GDPR (chiefly the definition of consent).

Further reading

Relevant provisions in the GDPR – See Recital 47 and Article 21 (the right to object) and Article 94 (repeal of data protection directive)
External link

Further reading – ICO guidance

Right to object

Guide to PECR

Direct Marketing guidance

Can we use legitimate interests for our business to business contacts?

Yes, it is likely that much of this type of processing will be lawful on the basis of legitimate interests, but there is no absolute rule here and you need to apply the three-part test.

You are still processing personal data when you are using and holding the names and details of your individual contacts at other businesses. You must have a lawful basis to process this personal data.

You can consider using legitimate interests as your lawful basis for such processing. However you need to identify your specific interest underlying the processing and ensure that the processing is actually necessary for that purpose.

Assuming you can meet these first two parts of the three-part test, you also need to consider the balancing test. You may find it is straightforward as business contacts are more likely to reasonably expect the processing of their personal data in a business context, and the processing is less likely to

have a significant impact on them personally.

Example

Individuals attend a business seminar and the organiser collects business cards from some of the delegates.

The organiser determines that they have a legitimate interest in networking and the growth of their business. They also decide that collecting delegate contact details from business cards is necessary for this purpose.

Having considered purpose and necessity the organiser then assesses that the balance favours their processing as it is reasonable for delegates handing over business cards to expect that their business contact details will be processed, and the impact on them will be low. The organiser also ensures that it will provide delegates with privacy information including details of their right to object. The organiser subsequently collates the contact details of the delegates and adds them to their business contacts database.

If you intend to process the personal data of your business contacts you need to remember that individuals' rights, including the right to be informed, still apply.

Further reading – ICO guidance

Individuals' rights

Can we use legitimate interests to process children's personal data?

The GDPR does not ban you from relying on legitimate interests as your lawful basis if you are processing children's personal data. However Article 6(1)(f) specifically highlights children's personal data as requiring particular protection.

If you choose to rely on legitimate interests for processing children's personal data you have a responsibility to protect them from risks that they may not fully appreciate and from consequences that they may not envisage. You must ensure their interests are adequately protected and that there are appropriate safeguards.

A legitimate interests assessment may be a useful tool to help you ensure that you properly consider the children's interests. However, you need to give extra weight to their interests and you need a more compelling interest to justify any potential impact on children on this basis.

Further Reading

Relevant provisions in the GDPR – See Articles 6(1)(f) and Recital 38
External link

Further reading – ICO guidance

Children and the GDPR

Can we use legitimate interests to disclose data to third parties?

You may be able to lawfully disclose data on the basis of legitimate interests. These might be your own interests, or the interests of the third party receiving the data, or a combination of the two.

Your focus is on justifying your disclosure when you carry out the three-part test. Although the third party's intentions and interests are directly relevant, your focus is on whether the disclosure itself is justified for that purpose. The third party is responsible for ensuring their own further processing is fair and lawful, including carrying out their own three-part test if they plan to rely on legitimate interests as their basis for processing.

What about special category data?

You can still consider legitimate interests as your lawful basis for processing special category data, but even if it applies you also need a special category condition under Article 9. If you are unable to meet a condition you are not able to process the special category data, even if legitimate interests applies under Article 6.

There is no special category condition equivalent to legitimate interests, as the conditions are designed to be more specific to the purpose of the processing. But there are ten special category conditions to choose from in the GDPR (supplemented by Schedule 1 of the Data Protection Bill). You should consider whether any of these conditions fit the circumstances.

If you are processing special category data, in most cases the sensitive nature of this data means there are greater risks to the interests and rights or freedoms of the individual. Therefore you may need to ensure that you put in place more robust safeguards to mitigate any impact or risks to the individual as a result of your processing, or that there is a more compelling justification.

You are also more likely to need to consider carrying out a DPIA.

Further reading – ICO guidance

Special category data

When should we avoid choosing legitimate interests?

There are a number of factors which might indicate that legitimate interests is unlikely to be an appropriate lawful basis for your processing. For example, you should avoid choosing legitimate interests if:

- you are a public authority and the processing is to perform your tasks as a public authority;

- your processing does not comply with broader legal, ethical or industry standards;
- you don't have a clear purpose and are keeping the data 'just in case' (in this case your processing is not compliant on any basis);
- you could achieve your end result without using personal data;
- you don't want to take full responsibility for protecting the interests of the individual, or would prefer to put the onus onto the individual;
- you intend to use the personal data in ways people are not aware of and do not expect (unless you have a more compelling reason that justifies the unexpected nature of the processing);
- there's a risk of significant harm (unless you have a more compelling reason that justifies the impact);
- you're not confident on the outcome of the balancing test;
- you would be embarrassed by any negative publicity about how you intend to use the data; or
- another lawful basis more obviously applies to a particular purpose. Although in theory more than one lawful basis may apply to your processing, in practice legitimate interests is unlikely to be appropriate for any processing purpose where another basis objectively applies.

Example

A retailer operates a loyalty scheme. Individuals sign up in order to be part of the scheme and collect loyalty points, providing personal data in return for special offers. The retailer will be processing personal data for different purposes and wants to use legitimate interests as their lawful basis.

The purposes for processing the personal data are:

1. to calculate the amount of vouchers and post vouchers to the individual;
2. to profile the interests of individuals to post and email targeted discounts;
3. for data analytics so it can improve its products and services.

The terms and conditions of the loyalty scheme amount to a contract. The scope of the services will dictate what processing can be said to be 'necessary for the contract'.

Purpose 1. is a core service, so processing for that purpose is necessary for the contract. As the processing is objectively lawful on the basis of contract, legitimate interests would not be appropriate. This is because basing the processing on legitimate interests over contract means that individuals would be deprived of their data portability rights.

Purpose 2. is not a core service, and is actually direct marketing to which the individual has the right to object. Processing for this purpose is not necessary for the contract. The retailer may choose to consider consent or legitimate interests for this processing.

Purpose 3. again is not a core service and so is not necessary for the contract. The retailer may choose to consider consent or legitimate interests for this processing. An alternative approach is for this personal data to be anonymised before it is used for data analytics.

What are the alternatives?

You must have a lawful basis in order to process personal data. Legitimate interests is one of the six lawful bases but there are alternatives. The other lawful bases are in brief:

- **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

You should always choose the basis that is most appropriate to the particular circumstances.

Further reading – ICO guidance

Lawful basis for processing

How do we apply legitimate interests in practice?

In detail

What do we need to do in practice?

You need to assess each part of the three-part test, and document the outcome so that you can demonstrate that legitimate interests applies. We refer to this as a 'legitimate interests assessment' or LIA (although this terminology does not itself appear in the GDPR).

An LIA is a type of light-touch risk assessment based on the specific context and circumstances of the processing.

You need to record your LIA and the outcome. There is no specific requirement in the GDPR for you to do this. However, in practice you are likely to need an audit trail of your decisions and justification for processing on the basis of legitimate interests.

There is no one-size-fits-all approach to an LIA. Sometimes your LIA might be quite short, but in other situations it may be much more detailed, or identify the need for a DPIA.

Other resources

Sample LIA template (Word)

Further Reading

Relevant provisions in the GDPR – See Article 5(2)
External link

Why do we need to do an LIA?

There is no obligation in the GDPR to do an LIA, but it is best practice to conduct one and it is difficult to meet your obligations under the accountability principle without it.

The LIA encourages you to ask yourself the right questions about your processing and objectively consider what the reasonable expectations of the individuals are and any impact of the processing on them.

Conducting an LIA helps you ensure that your processing is lawful. It helps you to think clearly and sensibly about your processing and the impact it could have on the individual.

Recording your LIA also helps you demonstrate compliance with the principles and appropriate organisational measures in line with your accountability obligations under Articles 5(2) and 24.

What's the process for an LIA?

As your LIA determines if the legitimate interests basis applies, you must perform it before you start processing the data. You cannot start processing the data then retrospectively try and apply legitimate interests. Your processing is unlawful without a lawful basis, and this will lead to inevitable breaches of transparency and accountability requirements.

There's no defined process, but you should approach the LIA by following the three-part test:

1. The purpose test (identify the legitimate interest);
2. The necessity test (consider if the processing is necessary); and
3. The balancing test (consider the individual's interests).

The LIA doesn't have to take any particular form, although you can use our template if you find it helpful. However, you need to address each part of the three-part test and record the outcome. You should record all the relevant factors, whether or not they support your conclusion, as this shows that you have taken everything into account prior to making your decision.

1. How do we do the purpose test?

You need to identify your purpose and decide whether it counts as a legitimate interest. Be as specific as possible, as this helps you when it comes to the necessity and balancing tests.

You should ask:

- Why do you want to process the data?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- What is the intended outcome for individuals?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice?
- Are there any ethical issues with the processing?

You should also check whether you are using data for one of the following purposes (in which case the GDPR specifically says that these are legitimate interests, and, depending on the circumstances, your LIA could be quite brief):

- fraud prevention (to the extent strictly necessary);

- network and information security (to the extent strictly necessary); or
- indicating possible criminal acts or threats to public security.

Note that although intra-group administrative transfers and marketing are mentioned in the GDPR as potential legitimate interests, you are likely to need a more detailed LIA and cannot assume that this purpose is enough on its own to help justify your processing. For more information, see the section on When can we rely on legitimate interests?.

Example

Lenders share data with Credit Reference Agencies (CRAs) about the payments made by an individual on an account. That data is then shared with any other lender that the individual makes an application to, so they can assess the individual's ability and inclination to repay a loan.

- The lender wants to accurately assess the likelihood that they will get back the money they lend out.
- The benefit is to minimise the risk of bad debts and ensure that the lender makes sustainable lending decisions to achieve a reasonable overall rate of return.
- It is also in the interests of the individual making the application that lenders make responsible lending decisions and don't allow them to become overburdened with debt they can't afford.
- Finally, it is in the interests of the public that lenders can make accurate risk assessments when making lending decisions. Without this, lenders may be less willing to lend, or at least lend at a reasonable interest rate.
- These benefits are vital to the proper functioning of the credit system.
- The intended outcome for the individual is that they will either be granted or refused credit on the basis of their ability to repay.
- The lenders comply with relevant consumer credit laws and standards.

The lenders have demonstrated a clear and specific legitimate interest, and have a good foundation for demonstrating necessity and objectively considering the balance of interests.

2. How do we do the necessity test?

You must consider carefully whether the processing is actually necessary for the purpose you have identified in step one.

You need to ask:

- Will the processing actually help you achieve your purpose?
- Is the processing proportionate to that purpose, or could it be seen as using a sledgehammer to crack a nut?
- Can you achieve your purpose without processing the data, or by processing less data?
- Can you achieve your purpose by processing the data in another more obvious or less intrusive way?

Be honest in your consideration of whether the processing is necessary. If on the face of it there are potentially other less intrusive alternatives you need to be clear in your LIA why these are not reasonable alternatives.

If you find it difficult to explain how the processing helps achieve your objective, or there are many alternative methods which simply aren't your chosen business model, you may need to go back to step one and be more specific about your purpose. A clearly defined purpose should make the necessity test easier to navigate.

3. How do we do the balancing test?

You need to consider the interests and fundamental rights and freedoms of the individual, and whether these override the legitimate interests you have identified.

There is no exhaustive list of what you should take into account when conducting the balancing test. However you should as a minimum consider:

- the **nature of the personal data** you want to process;
- the **reasonable expectations** of the individual; and
- the **likely impact** of the processing on the individual and whether any safeguards can be put in place to mitigate negative impacts.

Nature of the data

You need to think about the sensitivity of the personal data you intend to process. For example:

- Is it special category data?
- Is it criminal offence data?
- Is it another type of data that people are likely to consider particularly 'private', for example financial data?
- Are you processing children's data or data relating to other vulnerable individuals?
- Is it data about people in their personal or professional capacity?

The more sensitive or 'private' the data, the more likely the processing is to be considered intrusive or to create significant risks to the individual's rights and freedoms. For example, by putting them at risk of unlawful discrimination. You are likely to need a more compelling reason to use this type of data, and take particular care to put adequate safeguards in place.

In contrast, if the processing involves personal data which is considered less sensitive or private, such as that of individuals in their work capacity, then it may be that the impact is less (although you should still give some thought to the likely impact).

Example

An employer asks its employees to provide emergency contact details of a family member or friend in case they have an accident or become seriously ill at work.

It is not practical for the employer to have consent from the family or friends of all its employees in

order to process their contact details for the purposes of being used in an emergency. The employer therefore considers if the legitimate interests basis applies.

The employer considers that being able to contact an individual's designated family member or friend in an emergency is a legitimate interest as a responsible employer. It also notes that it is in the interests of the employee that a family member or friend knows about the emergency and likewise it is in the interests of nominated person to be told.

It decides that asking employees to provide the personal data of other individuals is necessary for this purpose and that there is no other reasonable way of achieving the purpose.

The employer goes on to consider the balancing test. It takes into account that the data that it will be processing is not sensitive (names and contact details) and determines that the impact of holding these details in case of an emergency is minimal. The employer decides that only its HR department will have access to the contact details and will ensure that these details can only be used in an actual emergency. It determines that the balance favours their legitimate interest in processing the data.

Reasonable expectations

You need to consider whether people will reasonably expect you to use their data in this way in the particular circumstances. You should consider all relevant factors, including:

- Do you have an existing relationship with the individual? If so, what is the nature of that relationship?
- How have you used their data in the past?
- Did you collect data directly from the individual?
- What did you tell individuals at the time?
- If you obtained the data from a third party, what did they tell individuals about reuse of the data by third parties for other purposes?
- How long ago was the data collected? Are there any changes in technology or other context since that time that would affect current expectations?
- Is your intended purpose and method obvious or widely understood?
- Are you intending to do anything new or innovative?
- Do you have any actual evidence about expectations, eg from market research, focus groups or other forms of consultation?
- Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

This is an objective test. You do not have to show that every individual does in fact expect you to use their data in this way. Instead, you have to show that a reasonable person would expect the processing in light of the particular circumstances.

If your purpose and method of processing is not immediately obvious and there is the potential for a range of reasonable opinions about whether people would expect it, you may wish to carry out some form of consultation, focus group or market research with individuals to demonstrate expectations and support your position. If there are pre-existing studies in regard to reasonable expectations in a particular context, you may be able to draw on these as part of your determination of what individuals

may or may not expect.

Impact and safeguards

You need to consider the potential impact on individuals and any damage that your processing might cause.

Firstly, you should consider whether your processing is of a type inherently likely to result in a high risk to individuals' rights and freedoms. If so, you need to do a DPIA, which can also function as your LIA. If you do a DPIA, there is no need to do a separate LIA as it covers the same ground in more detail. You can use our DPIA screening checklist to identify whether the processing is of a type likely to result in high risk.

If you decide you do not need to do a DPIA, you still need to do a lighter-touch risk assessment to consider whether your processing might cause any harm to individuals' interests, rights and freedoms, even if this falls short of a high risk. You should in particular think about whether your processing might contribute to:

- a barrier to individuals exercising their rights (including but not limited to privacy rights);
- a barrier to individuals accessing services or opportunities;
- any loss of control over the further use of personal data;
- physical harm;
- financial loss, identity theft or fraud; or
- any other significant economic or social disadvantage (such as discrimination, loss of confidentiality or reputational damage).

You should look at both the likelihood and severity of any harm.

If you identify the potential for a high risk (either due to a chance of severe harm or a high likelihood of some harm), you need a much more compelling legitimate interest to satisfy the balancing test. You need to demonstrate that your legitimate interests can override a serious impact. This also triggers the need for a DPIA to assess those risks in more detail, even if you had not hit a specific trigger on the screening checklist.

If you identify a lower risk of some harm, you need to weigh this against the potential benefits of the processing.

You may also wish to consider if there are any safeguards that you could put in place to reduce or mitigate this risk. For example could you collect less data, or provide individuals with an opt-out?

Example

A retailer wants to send offers by post to its customers. Its product order form contains the following statement:

'We will send you information about our special offers to your billing address. If you don't want to hear about our offers please tick here o'

The retailer balances the interests of its customers against its legitimate interests in sending postal

marketing to existing customers to improve sales. Customers are likely to reasonably expect that they may receive some marketing material from the retailer as the retailer has provided a clear indication that this processing will occur. The impact on the individual is minimal. However by giving its customers a clear opportunity to opt out of this processing, the retailer has also put in a safeguard to ensure the individual retains control over their data and can easily exercise their right to object.

You may find that building in appropriate safeguards can change the balance and mean that the individual's interests no longer override your interests. However you should be aware that safeguards do not always justify the processing.

Providing an opt-out to individuals as part of using legitimate interests should not be confused with using consent as your lawful basis. Failure to opt out does not demonstrate affirmative consent.

Further Reading

Relevant provisions in the GDPR – See Recital 47 and Article 35 (DPIAs)
External link

Further reading – ICO guidance

Data protection impact assessments

Consent

How do we decide the outcome?

You need to weigh up all the factors identified during your LIA for and against the processing, and decide whether you still think your interests should take priority over any risk to individuals. This is not a mathematical exercise and there is an element of subjectivity involved, but you should be as objective as possible.

You must be confident that you can show why the benefits of the processing justify any risks you have identified. The more significant the risks, the more compelling your justification must be.

Sometimes the outcome very obviously weighs in one direction in which case making the decision should be straightforward.

Example

A company is deciding whether to dismiss one of its employees for misconduct. The company decides that it needs advice about employment law and wants to send details of the employee's alleged misconduct to its external legal advisors.

Purpose test: the company needs to be able to manage the performance of its workforce and ensure employees act appropriately. It also needs to ensure that any action it takes is in accordance with its employment law obligations. This is in the legitimate interest business interests of the company. It is also in the legitimate interests of employees that the company acts fairly and within the law in its dealings with employees.

Necessity test: it is necessary to obtain external legal expertise about the alleged misconduct and the relevant legal framework for this purpose. Only the personal data that is relevant to the allegations will be shared with its legal advisors, subject to professional confidentiality obligations.

Balancing test: the data concerns the individual's professional life rather than private life. There is a clearly defined employer-employee relationship and employees would reasonably expect the company to process details of professional conduct to manage performance, and to seek legal advice when dealing with potential dismissals. Whilst the sharing of the data might contribute to significant harm to the individual if the advice supports dismissal, it should also help to ensure that the decision is not arbitrary or unlawful. The data is also shared subject to professional confidentiality obligations, which provides a safeguard against other risks or loss of control over the data.

The outcome for the company having considered all the relevant factors is that the employee's interests do not outweigh its legitimate interests in obtaining legal advice, and processing is lawful on the basis of these legitimate interests.

In other cases you may find the outcome is harder to determine. If you are not sure, it may be safer to look for another lawful basis. Legitimate interests is not often the most appropriate basis for processing which is unexpected or high risk.

Further reading – ICO guidance

Lawful basis for processing

What happens next?

If you have conducted your LIA and decided to rely on legitimate interests as your lawful basis, you should not assume that this is where your responsibilities end.

Keep your LIA under regular review. If anything significant changes – such as the purpose, nature or context of the processing – that may affect the balance between you and the individual you should revisit your LIA and refresh it as appropriate.

For example if a new and unforeseen impact of your processing comes to light you need to revisit your LIA and the balancing test, and perhaps consider if any further safeguards are needed.

If your LIA concludes that the impact on individual overrides your legitimate interests, then you are not able to process the data for that particular purpose using the legitimate interest basis. You may be able to consider another lawful basis instead.

If it's a borderline call and you're not confident that your interests justify the impact on individuals, then

you may also wish to look for other lawful basis. For example you may wish to consider if consent is appropriate, to give the individuals full control over the use of their data.

If your LIA identifies potential high risks to the rights and freedoms of the individual you need to go on to do a DPIA to assess the risks and potential safeguards in more detail.

Further Reading

Relevant provisions in the GDPR – See Article 6 (lawful bases) and Article 35(7)(a) (DPIAs)
External link

Further reading – ICO guidance

Consent

How does this tie in to DPIAs?

There are similarities between an LIA and a DPIA. Both involve considering the purpose of the processing, identifying and assessing risk, and considering possible safeguards.

However an LIA is intended as a simpler form of risk assessment, to prompt you to properly identify your purpose and think about the impact on individuals. You need to do an LIA in any case where you are considering using the legitimate interests basis, whether or not there are any particular reasons for concern. There are no absolute requirements for content or process, as long as you are confident that your processing is justifiable.

By contrast, a DPIA is a much more in-depth end-to-end process, with more specific minimum requirements as to content and process. You only need to do a DPIA if you identify that the processing is of a type considered likely to result in high risk (see our DPIA screening checklist), but you need to do it irrespective of what lawful basis you are considering. If you cannot mitigate risks, you need to consult the ICO before you can start processing.

However, there is some overlap between the two and you should recognise this in your processes. In practice, it is sensible to incorporate the DPIA screening checklist for types of processing likely to result in high risk as part of your balancing test as a simple way of identifying risks to individuals.

An LIA is also a potential trigger for a DPIA. If your LIA identifies the potential for high risks to individuals' rights and freedoms (either because of the severity or likelihood of the harm) then you are likely to need to carry out a DPIA.

You may be able to build on or adapt your LIA into your DPIA. If you have not yet carried out an LIA, there is no need to do both. You can use your DPIA instead of an LIA to demonstrate how legitimate interests applies, as it covers the same ground in more detail.

Further reading – ICO guidance

Data protection impact assessments

Further Reading

Relevant provisions in the GDPR – See Article 35 (DPIAs) (external link)
External link

What else do we need to consider?

In detail

- What do we need to tell people?
- What if our purposes change?
- What rights will individuals have?

What do we need to tell people?

You must tell individuals:

- what your purpose for processing personal data is;
- that you are relying on legitimate interests as your lawful basis; and
- summarise what the relevant legitimate interests are.

You need to include this in your privacy information. You also need to ensure that you actively communicate this information to the individuals.

Further reading – ICO guidance

Right to be informed

Further Reading

Relevant provisions in the GDPR – See Articles 13(1)(c) and 13(1)(d), Articles 14(1)(c) and 14(2)(b)
External link

What if our purposes change?

If your purposes change over time or you have a new purpose which you did not originally anticipate, you may be able to continue processing for that new purpose on the basis of legitimate interests as long as your new purpose is compatible with your original purpose.

Information on how to assess compatibility can be found in our lawful basis for processing guidance.

A compatibility assessment is likely to look at similar factors to an LIA because it also needs to consider your purpose, reasonable expectations, impact on individuals and possible safeguards. We would therefore recommend that you always conduct a fresh LIA as a matter of good practice as this either helps you demonstrate compatibility or else ensure that legitimate interests applies to the new processing on its own merits.

Remember that even if the processing for a new purpose is lawful on the basis of legitimate interests,

you still need to consider whether it is fair and transparent, ensure it complies with the purpose limitation principle (or satisfies an exemption from that principle), and give individuals information about the new purpose.

Further Reading

Relevant provisions in the GDPR – See Articles 6(4), and Recital 50 (external link)
External link

What rights will individuals have?

Most of the rights afforded to individuals are available if you are relying on legitimate interests as your lawful basis.

However, if you rely on legitimate interests then the right to data portability does not apply to any personal data being processed on that basis. This means that you do not need to comply with portability requests from individuals. Remember that you cannot choose legitimate interests in order to frustrate portability requests if the basis of necessary for performance of a contract applies, as this would be an unwarranted impact on individuals' rights.

You should remember that individuals do have the right to object to processing on the basis of legitimate interests. However this is not an absolute right, and you may be able to show that the processing should continue (unless you are processing for direct marketing purposes).

In order to continue processing despite an objection you must be able to demonstrate compelling legitimate grounds. Demonstrating compelling legitimate grounds is more than simply repeating the balancing test, as you need a stronger justification to override a specific objection and you need to consider the particular grounds that the individual has raised.

If you are relying on legitimate interests for direct marketing purposes, you need to stop the processing if the individual objects. This includes profiling to the extent that it is for the purposes of direct marketing. The right to object to processing for direct marketing purposes is absolute and the individual can exercise this right at any time. No compelling legitimate interests overrides this right to stop direct marketing.

Further reading – ICO guidance

Right to data portability

Right to object

Further Reading

Relevant provisions in the GDPR – See Article 20, and Recitals 68 (data portability), and Articles 21(1), 21(2), 21(3) and Recital 69 (the right to object)
External link